FRAUDE DEL CEO

El fraude del CEO tiene como objetivo engañar a empleados que tienen acceso a los recursos económicos para que paguen una factura falsa o haga una transferencia desde la cuenta de la compañía.

¿CÓMO LO HACEN?

Un estafador llama o envía correos electrónicos haciéndose pasar por un alto cargo de la compañía (p. ej. el Director General).

Conoce bien cómo funciona la organización.

Solicita que se haga un pago urgente.

Usa expresiones como "Confidencialidad", "La compañía confía en ti", "Ahora mismo no estoy disponible".

A menudo se solicita un pago internacional a bancos fuera de Europa.

El empleado transfiere los fondos a una cuenta controlada por el estafador.

Las instrucciones sobre cómo proceder puede darlas posteriormente una tercera persona o por correo electrónico.

Solicita al empleado que no siga los procedimientos de autorización habituales.

Hace referencia a una situación delicada (p. ej. una inspección fiscal, una fusión o una adquisición).

¿QUÉ SEÑALES TE ALERTARÁN?

- Llamada telefónica o correo no solicitado
- Presión y carácter de urgencia
- Comunicación directa con un alto cargo con el que normalmente no estás en contacto
- Solicitud fuera de lugar que contradice los procedimientos internos
- Solicitud de absoluta confidencialidad
- Amenazas, comentarios aduladores o promesas de recompensa

¿QUÉ PUEDES HACER?

COMO EMPRESA

Sé consciente de los riesgos y asegúrate de que **los empleados estén también concienciados.**

Anima a tus equipos a ser **precavidos cuando les soliciten un pago.**

Implanta protocolos internos para los pagos.

Implanta un procedimiento para verificar la legitimidad de las solicitudes de pago recibidas por correo.

Establece **procedimientos** para gestionar el fraude.

Revisa el contenido del portal web de tu empresa, **limita la información y sé cauteloso** en las redes sociales.

Mejora y actualiza la seguridad de tus sistemas.

Contacta siempre con la policía en caso de intento de fraude, incluso si has logrado evitarlo.

COMO EMPLEADO

Respeta estrictamente los procedimientos de seguridad vigentes para los pagos y las compras. **No te saltes ningún paso y no cedas a la presión.**

Revisa siempre con cuidado las direcciones de correo cuando manejes información delicada o hagas transferencias.

En caso de duda sobre una orden de transferencia, **consulta a un compañero experto.**

No abras nunca enlaces o adjuntos sospechosos recibidos por correo. Ten especial cuidado al consultar tu correo personal en los ordenadores de la empresa.

Limita la información y sé cauto en las redes sociales.

No compartas información sobre el organigrama, la seguridad y los procedimientos de tu compañía.

Si recibes un correo o una llamada sospechosa, **informa siempre al departamento de informática.**

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa

ESTAFA DE INVERSIÓN

Las "estafas de inversión" más comunes pueden incluir oportunidades de inversión lucrativa en acciones, bonos, criptomonedas, metales raros, inversiones en el extranjero o energía alternativa.

¿QUÉ SEÑALES TE ALERTARÁN?

- Te prometen ganancias rápidas y te aseguran que la inversión es segura.
- La oferta es válida solo durante un tiempo limitado.
- Recibes continuamente llamadas no solicitadas.
- La oferta está disponible solo para ti y te piden que no se lo digas a nadie.

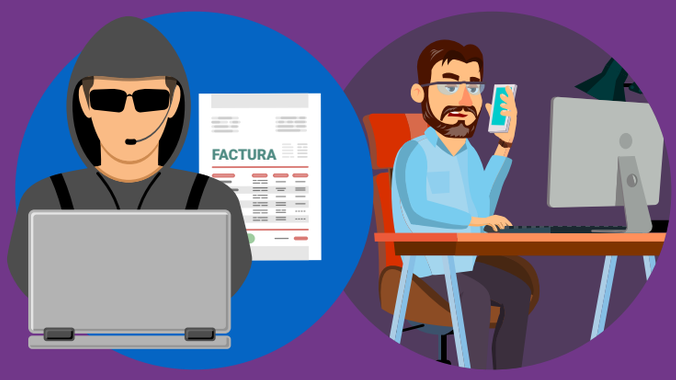
¿QUÉ PUEDES HACER?

- **Obtén siempre asesoramiento financiero** antes de entregar dinero o hacer una inversión.
- **Rechaza llamadas** no solicitadas relacionadas con oportunidades de inversión.
- **Sospecha** de las ofertas que prometen una inversión segura, retornos garantizados y grandes ganancias.
- **Mantente alerta.** Si ya te han estafado antes, es probable que te mantengan como objetivo o que vendan tus datos a otros delincuentes.
- Si sospechas, **contacta con la policía.**

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa

EL FRAUDE DE FACTURAS



¿CÓMO LO HACEN?

- Alguien que dice ser un representante de un suministrador, proveedor o un acreedor, contacta con una empresa o negocio.
- Pueden combinar varias formas de contacto: teléfono, carta, correo electrónico, etc.
- El estafador solicita que se cambien los datos bancarios para el pago de las próximas facturas. La nueva cuenta está controlada por el estafador.

¿QUÉ PUEDES HACER?

COMO EMPRESA

Asegúrate de que **los empleados están informados y conocen** este tipo de fraude y cómo evitarlo.

Forma al personal responsable de pagar las facturas para que **verifique siempre que no haya irregularidades.**

Implementa un **procedimiento para verificar** la legitimidad de las solicitudes de pago.

Revisa la información publicada en la web de la empresa, en especial la de suministros y proveedores. Asegúrate de que tu personal no comparte datos de la empresa en redes sociales.

COMO EMPLEADO

Verifica las peticiones que parezcan ser de tus acreedores, en especial si piden cambiar los datos bancarios para próximas facturas.

Para los pagos que superen un límite definido, **establece un procedimiento para confirmar** la cuenta y el destinatario correctos (p. ej. una reunión con la empresa).

No uses los datos de contacto de una carta, fax o correo que solicita un cambio. En lugar de estos, utiliza los de **correspondencias anteriores.**

Cuando se pague una factura **envía un correo al destinatario para informarle**. Incluye el nombre del banco beneficiario y los últimos cuatro dígitos de la cuenta para garantizar la seguridad.

Establece un **Punto de Contacto Único** con las empresas a las que realizas pagos habitualmente.

Evita compartir información sobre tu empresa en redes sociales.

Contacta siempre con la policía en caso de intento de fraude, incluso si has logrado evitar el engaño.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa

ESTAFAS EN COMPRAS POR INTERNET

Puedes encontrar buenas ofertas en internet... ¡pero ten cuidado con las estafas!

¿QUÉ PUEDES HACER?

- Cuando sea posible **utiliza páginas web de comercios de ámbito nacional:** es más probable que puedan resolver cualquier problema.
- **Investiga un poco:** busca referencias antes de comprar.

- **Paga con tarjeta:** tienes más posibilidades de recuperar tu dinero.
- **Paga a través de pasarelas de pago seguro:** ¿Están solicitando una transferencia o un giro bancario? ¡No te fíes!
- Paga desde una **conexión segura a internet:** evita el uso de wifi público gratuito o abierto.
- **Paga desde un dispositivo seguro:** mantén tu sistema operativo y tus aplicaciones de seguridad actualizados.
- Ten cuidado con las ofertas sorprendentes o los productos milagrosos: **si suena demasiado bien, ¡probablemente es un engaño!**
- ¿Un anuncio en una ventana emergente te avisa de que has ganado un premio? **Cuidado**, puedes ganarte un programa malicioso.
- Si el producto no llega, contacta con el vendedor. Si no te contesta, **contacta con tu banco.**

Si sospechas que puede ser un intento de fraude, informa a la policía, incluso si has logrado evitar el engaño.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa

'PHISHING' BANCARIO POR CORREO ELECTRÓNICO

'Phishing' se refiere a correos electrónicos fraudulentos que engañan a los destinatarios para que compartan su información personal, financiera o de seguridad.

¿CÓMO LO HACEN?

Estos correos electrónicos:

Pueden parecer idénticos al tipo de correspondencia que envían los bancos reales.

Copian los logotipos, el diseño y el tono de los correos electrónicos reales.

Te piden que descargues un documento adjunto o hagas clic en un enlace.

Usan un lenguaje que transmite un sentido de urgencia.

Los ciberdelincuentes asumen que las personas están ocupadas; a simple vista, estos correos electrónicos falsos parecen ser legítimos.

Ten cuidado cuando uses un dispositivo móvil. Puede ser más difícil detectar un intento de 'phishing' desde tu tableta o móvil.

¿QUÉ PUEDES HACER?

- **Mantén tus aplicaciones actualizadas,** incluyendo navegador, antivirus y sistema operativo.
- Presta especial atención si un correo electrónico de tu 'banco' te solicita información confidencial (p. ej. la contraseña de tu cuenta bancaria).
- **Revisa el correo con cuidado:** compara la dirección con los mensajes auténticos de tu banco. Comprueba si existen errores de ortografía o de gramática.
- **No respondas a un correo electrónico sospechoso,** reenvíalo a tu banco escribiendo tú la dirección real.
- **No hagas clic en el enlace o descargues el archivo adjunto, escribe la dirección real de tu banco en el navegador.**
- En caso de duda, **comprueba la información** entrando en la página web de tu banco o por teléfono.

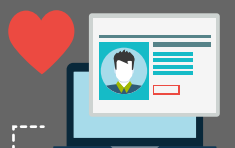
#Ciberestafa

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

ESTAFA AMOROSA

Los estafadores buscan victimas en páginas web de contactos, en redes sociales o por correo electrónico.

¿QUÉ SEÑALES TE ALERTARÁN?



Alguien que has conocido hace poco en internet manifiesta intensos sentimientos por ti y te pide chatear por privado.

Sus mensajes a menudo están mal escritos y son confusos.

Su perfil en internet no coincide con lo que cuenta.

Te puede pedir que le envíes fotos o videos íntimos tuyos.

Primero trata de ganar tu confianza. Después te pide dinero, regalos o los datos de tu cuenta corriente o tarjeta de crédito.

Si no le envías dinero, puede tratar de chantajearte. Si se lo envías, te pedirá más.

¿ERES UNA VÍCTIMA?

¡No te sientas avergonzado!
Cesa inmediatamente todo contacto.
Si es posible, guarda las comunicaciones (mensajes del chat).
Presenta una denuncia a la policía.
Informa a la plataforma 'online' donde conociste al estafador.
Si has facilitado datos de tu cuenta, contacta con tu banco.

¿QUÉ PUEDES HACER?

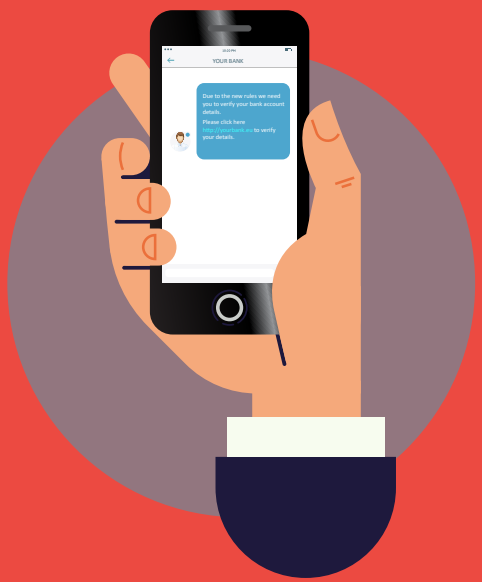
- **Ten mucho cuidado** con la información que compartes en las redes sociales y en las páginas de contactos.
- **Considera siempre los riesgos.** Los estafadores están en las páginas más respetables.
- **Actúa con cabeza** y tantea con preguntas.
- **Investiga** la fotografía y el perfil de la persona para averiguar si se ha utilizado en otros sitios.
- **Estate atento** a los errores ortográficos y gramaticales, historias incoherentes y excusas como que su cámara no funciona.
- **No compartas** nada que pueda comprometerte y sirva para chantajearte.
- Si aceptas veros en persona, **cuenta a tu familia y amigos** dónde vas a estar.
- **Ten cuidado si te piden dinero.** No lo envíes nunca ni proporciones los datos de tu tarjeta, cuenta bancaria, o copias de tu DNI.
- Evita enviar pagos por adelantado.
- **No transfieras dinero** en nombre de otra persona: el blanqueo de dinero es delito.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa

'SMISHING' BANCARIO POR SMS

El 'smishing' (combinación de las palabras SMS y 'phishing') es el intento de fraude para obtener información personal, financiera o de seguridad a través de un mensaje de texto.



¿CÓMO LO HACEN?

El mensaje de texto normalmente te pedirá que hagas clic en un enlace o que llames a un teléfono para "verificar", "actualizar" o "reactivar" tu cuenta. Pero... el enlace te lleva a una página web falsa, y el número de teléfono es el de un estafador que suplanta a una empresa.

¿QUÉ PUEDES HACER?

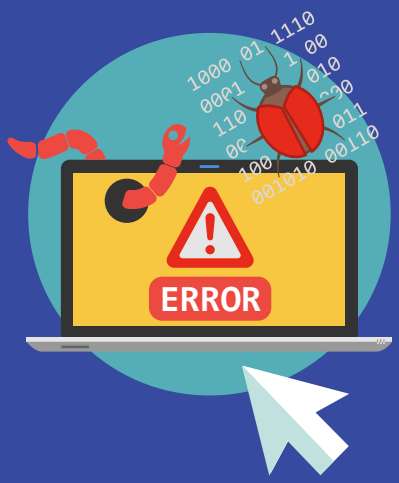
- **No hagas clic en enlaces, adjuntos o imágenes** que recibas en mensajes de texto no solicitados sin antes verificar el remitente.
- **No te apresures.** Tómate tu tiempo y haz las comprobaciones necesarias antes de responder.
- **Nunca respondas a un mensaje de texto** que te solicite tu PIN o la contraseña de tu banco, o cualquier otra credencial de seguridad.
- Si crees haber respondido a un 'smishing' y proporcionado tus datos bancarios, **contacta con tu banco de inmediato.**

EUROPOL EC3 European Cybercrime Centre · EBF · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa

BANCA ELECTRÓNICA FRAUDULENTA

Los 'phishing' bancarios vía correo electrónico suelen incluir enlaces que te redirigen a una página web fraudulenta, donde te solicitan tus datos personales y financieros.



¿QUÉ SEÑALES TE ALERTARÁN?

Las páginas web bancarias fraudulentas son casi idénticas a su equivalente legítimo. Estas páginas utilizan ventanas emergentes solicitando tus credenciales bancarias. Un banco real nunca las utilizaría.

Estas páginas web muestran habitualmente:

Urgencia: no encontrarás este tipo de mensajes en páginas web legítimas.

Ventanas emergentes: se utilizan para obtener información delicada sobre ti. No hagas clic ni introduzcas en ellas información personal.

Diseño poco cuidado: ten cuidado con las páginas web que tienen fallos en el diseño o faltas de ortografía.

¿QUÉ PUEDES HACER?

Nunca hagas clic en enlaces de correo electrónico que te redirijan a la web de tu banco.

Escribe siempre la dirección en el navegador o utiliza un enlace almacenado en tu lista de "favoritos".

Utiliza un navegador con **bloqueo de ventanas emergentes.**

Si hay algo importante que requiera tu atención, tu banco te alertará de ello **cuando accedas a tu banca electrónica.**

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa

'VISHING' BANCARIO POR TELÉFONO

'Vishing' (combinación de palabras "voz" y "phishing") es un fraude telefónico en el que los estafadores intentan engañar a la víctima para que divulgue información personal, financiera o de seguridad, o que transfiera dinero.

¿QUÉ PUEDES HACER?

- **Sé prudente** con las llamadas no solicitadas.
- **Anota el número desde el que te llaman,** y diles que les devolverás la llamada.
- Para confirmar su identidad, **busca el número de teléfono de la organización** y contacta con ellos directamente.
- **No confirmes la identidad de la persona que llama usando el número de teléfono que te han dado** (podría ser un número falso).
- Los estafadores pueden encontrar en internet información básica sobre ti (p.ej. en redes sociales). **No supongas que la llamada es legítima** solo porque tengan esos datos.
- **No compartas** el PIN de tus tarjetas o la contraseña de tu banco por internet. Tu banco nunca te solicitará esos datos.
- **No transfieras dinero a otra cuenta** cuando te lo pidan. Tu banco nunca te haría una petición así.
- Si crees que es una llamada falsa, **comunícaselo a tu banco.**

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa